(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－37589
（P2003－37589A）
(43)公開日　平成15年２月７日(2003.2.7)

(51)Int.Cl.[7]	識別記号	FI	テーマコード*(参考)
H04L 9/14		G11B 20/10	D 5C053
G11B 20/10			H 5D044
			311 5J104
	311		321Z
	321	H04L 9/00	641

審査請求　未請求　請求項の数22　ＯＬ　（全９頁）　最終頁に続く

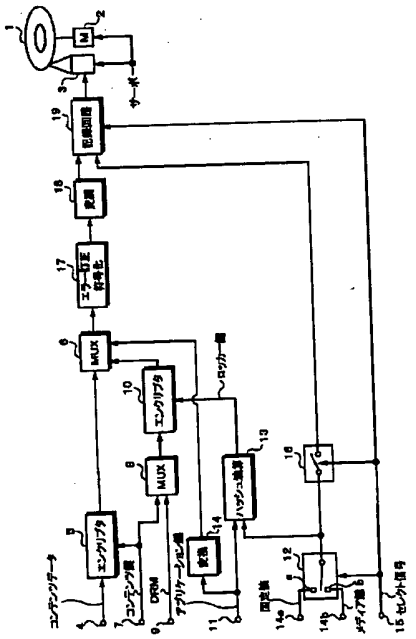
(21)出願番号　特願2001－226242(P2001－226242)
(22)出願日　平成13年７月26日(2001.7.26)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　猪口　達也
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082762
弁理士　杉浦　正知

最終頁に続く

(54)【発明の名称】　データ記録装置および方法、並びにデータ再生装置および方法

(57)【要約】
【課題】　メディアにバインドした鍵の代わりに固定値を使用して暗号化を行うことによって、新たなセキュリティシステムの導入を容易とする。
【解決手段】　記録すべきコンテンツデータがコンテンツ鍵を使用してエンクリプタ５によって暗号化される。コンテンツ鍵とＤＲＭがエンクリプタ１０においてロッカー鍵によって暗号化される。アプリケーション鍵とセレクタ１２で選択されたデータ（固定値またはメディア鍵）とのハッシュ値（ロッカー鍵）が演算される。アプリケーション鍵は、変換部１４において例えばスクランブルのようなデータ変換処理を受ける。暗号化されたコンテンツデータ、暗号化されたコンテンツ鍵およびＤＲＭ、並びに変換されたアプリケーション鍵がエラー訂正符号化器１７および変調部１８を介して記録回路１９に供給され、メディア鍵とセレクト信号と共に、光ピックアップ３によって光ディスク１に記録される。



【特許請求の範囲】

【請求項１】　コンテンツデータを暗号化して媒体に記録するデータ記録方法であって、
上記コンテンツデータを媒体にバインドさせない場合は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行うようにしたデータ記録装置。

【請求項２】　請求項１において、
上記コンテンツデータを媒体にバインドさせる場合には、上記媒体にバインドした鍵を使用して暗号化を行うようにしたデータ記録装置。

【請求項３】　請求項１において、
上記固定値は、媒体の所定の領域に記録されるデータであるデータ記録装置。

【請求項４】　請求項１において、
上記媒体にバインドした鍵は、媒体から読取可能であって、外部に出力されない識別情報であるデータ記録装置。

【請求項５】　請求項１において、
上記媒体にバインドさせるか否かを識別するための識別情報を媒体に記録するデータ記録装置。

【請求項６】　コンテンツデータを暗号化して媒体に記録するデータ記録方法であって、
上記コンテンツデータを媒体にバインドさせない場合は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行うようにしたデータ記録方法。

【請求項７】　請求項６において、
上記コンテンツデータを媒体にバインドさせる場合には、上記媒体にバインドした鍵を使用して暗号化を行うようにしたデータ記録方法。

【請求項８】　請求項６において、
上記固定値は、媒体の所定の領域に記録されるデータであるデータ記録方法。

【請求項９】　請求項６において、
上記媒体にバインドした鍵は、媒体から読取可能であって、外部に出力されない識別情報であるデータ記録方法。

【請求項１０】　請求項６において、
上記媒体にバインドさせるか否かを識別するための識別情報を媒体に記録するデータ記録方法。

【請求項１１】　コンテンツデータを暗号化して媒体に記録するデータ記録装置であって、
上記コンテンツデータを媒体にバインドさせる場合には、媒体にバインドした鍵を使用して暗号化を行い、
上記コンテンツデータを媒体にバインドさせない場合は、上記媒体にバインドした鍵に代えて固定値を使用して暗号化を行い、
上記固定値を使用して暗号化する場合では、再生環境を制限するための情報を記録するデータ記録装置。

【請求項１２】　請求項１１において、
上記再生環境を制限するための情報は、装置またはソフトウェアの識別子であるデータ記録装置。

【請求項１３】　コンテンツデータを暗号化して媒体に記録するデータ記録方法であって、
上記コンテンツデータを媒体にバインドさせる場合には、媒体にバインドした鍵を使用して暗号化を行い、
上記コンテンツデータを媒体にバインドさせない場合は、上記媒体にバインドした鍵に代えて固定値を使用して暗号化を行い、
上記固定値を使用して暗号化する場合では、再生環境を制限するための情報を記録するデータ記録方法。

【請求項１４】　請求項１３において、
上記再生環境を制限するための情報は、装置またはソフトウェアの識別子であるデータ記録方法。

【請求項１５】　暗号化されたコンテンツデータを媒体から再生する再生装置であって、
上記暗号化を復号する際に、上記暗号化が上記媒体にバインドされているか否かを判別し、判別結果に応じて上記暗号化に使用する鍵を切り換えることによって、上記コンテンツデータを再生するデータ再生装置。

【請求項１６】　請求項１５において、
上記暗号化が上記媒体にバインドされていない場合では、上記暗号化に使用する鍵として固定値を使用するデータ再生装置。

【請求項１７】　請求項１５において、
上記暗号化が上記媒体にバインドされている場合では、上記復号方法に上記媒体にバインドしている鍵を使用するデータ再生装置。

【請求項１８】　暗号化されたコンテンツデータを媒体から再生する再生方法であって、
上記暗号化を復号する際に、上記暗号化が上記媒体にバインドされているか否かを判別し、判別結果に応じて上記復号に使用する鍵を切り換えることによって、上記コンテンツデータを再生するデータ再生方法。

【請求項１９】　請求項１８において、
上記暗号化が上記媒体にバインドされていない場合では、上記復号に使用する鍵として固定値を使用するデータ再生方法。

【請求項２０】　請求項１８において、
上記暗号化が上記媒体にバインドされている場合では、上記復号に上記媒体にバインドしている鍵を使用するデータ再生方法。

【請求項２１】　暗号化されたコンテンツデータを媒体から再生する再生装置であって、
上記暗号化を復号する際に、上記暗号化が上記媒体にバインドされているか否かを判別し、判別結果に応じて上記暗号化に使用する鍵を切り換えることによって、上記コンテンツデータを再生し、
上記暗号化が上記媒体にバインドする場合には、再生環境を制限せず、上記暗号化が上記媒体にバインドしない場合では、再生環境を制限するデータ再生装置。

【請求項２２】　暗号化されたコンテンツデータを媒体から再生する再生方法であって、
上記暗号化を復号する際に、上記暗号化が上記媒体にバインドされているか否かを判別し、判別結果に応じて上記暗号化に使用する鍵を切り換えることによって、上記コンテンツデータを再生し、
上記暗号化が上記媒体にバインドする場合には、再生環境を制限せず、上記暗号化が上記媒体にバインドしない場合では、再生環境を制限するデータ再生方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、暗号化によってセキュリティを保つようにしたデータ記録装置および方法、並びにデータ再生装置および方法に関する。
【０００２】
【従来の技術】近年、音楽情報が記録されたＣＤ(Compact Disc)のディジタルデータをＭＰ３で圧縮したコンテンツがインターネットを介して配信されたり、ＣＤ－Ｒ(CD-Recordable)を使用してＣＤがコピーされたり、米Napster社が提供するピア・ツー・ピア型の音楽ファイルの交換サービスが広まっており、著作権保護（以下、適宜セキュリティと称する）の問題が大きくクローズアップされている。このため、近年提案されている新規なメディア（ＳＡＣＤ(Super Audio CD)、ＤＶＤ(Digital Versatile Disc またはDigital Video Disc)オーディオ、メモリカード、データプレイディスク等）では、コンテンツを暗号化し、セキュリティを保っている。例えばメモリカードは、フラッシュメモリを使用し、機器に着脱自在とされたもので、暗号化された音楽データをメモリカードに記録しようとすると、認証が行なわれ、認証が成立して初めて暗号化データを記録することが可能となる。
【０００３】また、データプレイディスクは、米DataPlay社の提案による小型光ディスク（直径３２ｍｍ）であり、著作権保護技術が採用されている。この技術は、暗号化とコンテンツの再生条件を制御する技術で構成される。著作権保護システムのみがアクセスできるディスク内周部の専用領域にコンテンツの暗号を解く「暗号化キー」とユーザによるアクセス条件を規定する「条件アクセスキー」が格納される。
【０００４】また、鍵情報そのものではなく、鍵情報を生成するのに不可欠な情報を再生専用領域（ＲＯＭ部分）に記録することが考えられている。例えばＤＶＤの不正コピー防止技術として、書き換え可能なＤＶＤの最内周部の再生専用領域（ＲＯＭ部分）にメディアＩＤを記録し、メディアＩＤとＭＫＢ(Media Key Block)のハッシュ値を鍵データとして暗号化されたコンテンツをそのディスクに記録することが提案されている。メディアＩＤは、ディスク毎に異なる値であり、ユーザが書き換えることができないので、たとえデータ部分を他の別の

ディスクに不正にコピーしても、メディアＩＤが元のディスクとは異なるので、そのデータ部分を復号することが不可能である。
【０００５】
【発明が解決しようとする課題】上述したような著作権保護対策がなされた新規メディアを利用するためには、新規なレコーダ／プレーヤを購入する必要がある。このことは、ユーザに新たな負担を生じさせるので、新規メディアが広く普及する妨げとなる。一方、既存のレコーダ／プレーヤに著作権保護対策を導入しようとしても、互換性の問題が生じたり、互換性をとるためにパーソナルコンピュータにインストールしたソフトウェアで暗号化を復号しようとすると、充分な著作権保護ができない問題があった。
【０００６】したがって、この発明の目的は、メディアにバインドした鍵を使用して暗号化する本格的なセキュリティ機能の導入を容易とすることが可能なデータ記録装置および方法、並びにデータ再生装置および方法を提供することにある。
【０００７】
【課題を解決するための手段】上述した課題を達成するために、請求項１の発明は、コンテンツデータを暗号化して媒体に記録するデータ記録方法であって、コンテンツデータを媒体にバインドさせない場合は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行うようにしたデータ記録装置である。請求項６の発明は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行うようにしたデータ記録方法である。
【０００８】請求項１１の発明は、コンテンツデータを暗号化して媒体に記録するデータ記録装置であって、コンテンツデータを媒体にバインドさせる場合には、媒体にバインドした鍵を使用して暗号化を行い、コンテンツデータを媒体にバインドさせない場合は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行い、固定値を使用して暗号化する場合では、再生環境を制限するための情報を記録するデータ記録装置である。請求項１３の発明は、固定値を使用して暗号化する場合では、再生環境を制限するための情報を記録するデータ記録方法である。
【０００９】請求項１５の発明は、暗号化されたコンテンツデータを媒体から再生する再生装置であって、暗号化を復号する際に、暗号化が媒体にバインドされているか否かを判別し、判別結果に応じて暗号化に使用する鍵を切り換えることによって、コンテンツデータを再生するデータ再生装置である。請求項１８の発明は、判別結果に応じて復号に使用する鍵を切り換えることによって、コンテンツデータを再生するデータ再生方法である。
【００１０】請求項２１の発明は、暗号化されたコンテンツデータを媒体から再生する再生装置であって、暗号

化を復号する際に、暗号化が媒体にバインドされているか否かを判別し、判別結果に応じて暗号化に使用する鍵を切り換えることによって、コンテンツデータを再生し、暗号化が媒体にバインドする場合には、再生環境を制限せず、暗号化が媒体にバインドしない場合では、再生環境を制限するデータ再生装置である。請求項２２の発明は、暗号化が媒体にバインドしない場合では、再生環境を制限するデータ再生方法である。

【００１１】この発明では、媒体にバインドしていないが、媒体にバインドした鍵と同様に暗号化の鍵として機能する固定値を使用することを可能とする。固定値を使用して暗号化されたコンテンツデータの記録された媒体は、媒体にバインドした鍵で暗号化されたコンテンツデータの記録された媒体と殆ど同一のセキュリティシステムで扱うことが可能となり、互換性を容易にとることができる。この発明は、媒体にバインドした鍵を使用する本格的セキュリティシステムの導入を容易とすることができる。

【００１２】

【発明の実施の形態】以下、この発明の一実施形態について説明する。この一実施形態は、光ディスクに対してこの発明を適用した例である。図１を参照して、記録装置の一例について説明する。図１において、参照符号１が光ディスク例えばＣＤ－ＲＷまたはＣＤ－Ｒと同様の記録可能な光ディスクを示す。この光ディスク１に対して記録されるコンテンツデータは、全て暗号化されるものと規定されている。したがって、暗号化を行なわない既存のドライブによって、光ディスク１を使用して記録および再生を行うことができない。

【００１３】図１に示す記録装置および後述する再生装置（図２）は、専用のハードウエアに限らず、パーソナルコンピュータとソフトウェアによって実現することが可能である。特に、セキュリティに関連する暗号化および復号化の処理をソフトウェアによって実現するようになされる。

【００１４】光ディスク１は、スピンドルモータ２によって、線速度一定または角速度一定で回転駆動される。光ディスク１にデータを記録し、光ディスク１に記録されたデータを読み出すために、光ピックアップ３が設けられている。光ピックアップ３が送りモータ（図示しない）によって光ディスク１の径方向に送られる。

【００１５】この一実施形態の光ディスク１は、記録に必要とされる出力レベルのレーザ光を照射することによってデータの記録が可能で、光ディスク１によって反射されたレーザ光の光量の変化を検出することによって再生可能な相変化型ディスクである。相変化記録材料からなる記録膜が被着される基板の材質は、例えばポリカーボネートであり、ポリカーボネートを射出成形することによって、基板上にグループと呼ばれるトラック案内溝が予め形成されている。このディスク基板上に形成されるグループは、予め形成する意味でプリグループとも呼ばれ、グループの間は、ランドと呼ばれる。通常、読取レーザ光の入射側から見て手前側がランドであり、遠い側がグループであると定義される。グループは、内周から外周へスパイラル状に連続して形成されている。なお、この発明は、記録可能であれば、相変化型光ディスクに限らず、光磁気ディスク、有機色素を記録材料として使用する追記形ディスクに対しても適用できる。

【００１６】グループは、光ディスク１の回転制御用と記録時の基準信号とするために光ディスクの径方向に蛇行（ウォブルと称する）している。データは、グループ内、またはグループおよびランドに記録される。さらに、グループのウォブル情報としてアドレス情報としての絶対時間情報を連続的に記録している。ＣＤ－Ｒディスク、ＣＤ－ＲＷディスクでは、グループのウォブル情報によって得られるアドレス情報としての絶対時間情報を参照して光ディスク１上の所望の書き込み位置を検索し、光ピックアップ３を移動させ、光ピックアップ３から光ディスク１に対してレーザ光を照射することによって、データをディスクに書き込むようにしている。

【００１７】このようなウォブリングしたグループを有する光ディスクは、以下のようにして製造される。マスタリング装置は、ディスク状のガラス原盤に塗布されたフォトレジスト膜にレーザ光を照射すると共に、レーザ光を径方向に偏向または径方向に振ることによって、アドレス情報、クロック情報等を有するウォブリンググループを形成する。レーザ光の照射によって露光されたフォトレジスト膜を現像することによってディスク原盤が作成され、ディスク原盤から電鋳処理によってスタンパが作成され、スタンパを用いて射出成形を行うことによって、上述したウォブルグループを有するディスク基板が成形される。このディスク基板に相変化型の記録材料をスパッタリング等の手法を用いて被着することによって光ディスクが作成される。

【００１８】図１に戻ると、記録すべきコンテンツデータ例えばオーディオおよび／またはビデオデータが入力端子４からエンクリプタ５に供給される。エンクリプタ５によって暗号化されたコンテンツデータがマルチプレクサ６に供給される。エンクリプタ５は、入力端子７からのコンテンツ鍵を使用してコンテンツデータに対して暗号化を施す。コンテンツ鍵は、マルチプレクサ８に対しても供給される。

【００１９】マルチプレクサ８に対してどのようにコンテンツを扱うかを指示する管理情報（ＤＲＭ(Digital Rights Management)と表記する）が入力端子９から供給される。例えばコピーの可否、コピー世代の管理の情報がＤＲＭに含まれている。マルチプレクサ８の出力データがエンクリプタ１０によって暗号化される。このエンクリプタ１０は、コンテンツ鍵とＤＲＭとを暗号化するためのものである。エンクリプタ１０から出力される暗

号化されたコンテンツ鍵およびＤＲＭがマルチプレクサ６に対して供給される。

【００２０】エンクリプタ１０に対しては、ロッカー鍵が供給され、ロッカー鍵によってコンテンツ鍵およびＤＲＭが暗号化される。ハッシュ演算部１３において、入力端子１１からのアプリケーション鍵とセレクタ１２で選択されたデータとのハッシュ値が演算される。このハッシュ値がロッカー鍵である。アプリケーション鍵は、メディアにバインドしていない鍵を意味し、ソフトウェアにより保持され、または、デバイスにより保持されている。アプリケーション鍵は、変換部１４において例えばスクランブルのようなデータ変換処理を受け、マルチプレクサ６に供給される。

【００２１】メディアにバインドしている鍵とは、そのメディアに記録されることによって、そのメディアに専用の鍵となるものを意味する。メディアにバインドしている鍵は、暗号化によるセキュリティ対策を行なわない既存のドライブによってメディアを再生した時には、読み取れないように、そのメディアに埋め込まれている。一方、セキュリティ対策を行う新規なドライブによって、メディアにバインドしている鍵を読み取ることが可能とされている。具体的には、ピット自身の変形またはピットの変位（ウォブリング）により表される鍵、ＥＦＭ変調における結合ビット（３ビット）を使用して表現された鍵、ディスク最内周領域に記録されたディスク固有のＩＤ等がメディアにバインドしている鍵である。新規なドライブは、メディアにバインドしている鍵を抽出し、抽出された鍵によって暗号化コンテンツを復号することができる。しかしながら、新規なドライブは、鍵自体を外部から知ることができないような対策がとられているのが普通であり、暗号化コンテンツと鍵とを不正にコピーしたメディアを作成することが不可能とされている。

【００２２】セレクタ１２は、第１の入力端子ａ、第２の入力端子ｂおよび出力端子を有し、入力端子ａと接続された入力端子１４ａには、固定値が供給され、入力端子ｂと接続された入力端子１４ｂには、メディア鍵が供給される。セレクタ１２は、例えばドライブ全体の動作を制御するソフトウェアに基づいて形成され、入力端子１５に供給されるセレクト信号によって制御される。セレクタ１２が選択したメディア鍵および固定値の一方がハッシュ演算部１３およびゲート１６に供給される。

【００２３】以下、固定値が選択されてデータが記録される光ディスク、すなわち、メディアにバインドしない光ディスクをタイプＡのディスクと適宜呼び、メディア鍵が選択されてデータが記録される光ディスク、すなわち、メディアにバインドした光ディスクをタイプＢのディスクと適宜呼ぶことにする。タイプＡおよびタイプＢの何れのディスクも、暗号化されたコンテンツデータが記録されるものである。

【００２４】ドライブ全体の動作を制御するソフトウェアは、ＣＤ－ＲＯＭ等のメディア、またはネットワークを介して配布されたものである。例えばメディア鍵が記録されたタイプＢのディスクを再生できる新規ドライブが未だ充分に普及していない段階では、固定値を選択するようにセレクタ１２を制御するセレクト信号をソフトウェアが発生するようになされる。その後、新規ドライブが充分に普及した段階では、メディア鍵を選択するようにセレクタ１２を制御するセレクト信号を発生するソフトウェアが配布される。なお、ユーザが所有しているドライブがタイプＡおよびタイプＢの何れのディスクに対応しているかに応じてセレクト信号を発生しても良い。

【００２５】固定値を使用して暗号化されたタイプＡのディスクは、既存のプレーヤで再生することができない。しかしながら、固定値を使用して暗号化を復号するデクリプタを既存のプレーヤに付加する変更を加えれば、タイプＡのディスクを再生することができる。メディア鍵の読取、ロッカー鍵およびコンテンツ鍵の生成等の処理に必要な構成を付加する必要がないので、比較的ローコストな構成が可能である。さらに、暗号化の復号をソフトウェア処理を行う場合では、タイプＡの光ディスクを既存のドライブで再生し、固定値を使用して復号することができる。この場合では、ドライブ側に対してハードウエアの変更を殆ど行なわずにタイプＡのディスクを再生することが可能となる。

【００２６】メディア鍵は、上述したメディア（ここでは光ディスク１）にバインドしている鍵を意味する。一方、固定値は、メディアにバインドしていない値である。例えば全て"1" のデータ、全て"0" のデータ、"101010・・・10"のような既知のパターンのデータが固定値である。さらに、光ディスク１の最内周側のリードイン領域の特定のアドレスに記録されている特定のデータを固定値として使用しても良い。例えばＴＯＣ(Table Of Contents)中のプログラムスタート時間、曲数のデータ、そのディスクの総演奏時間のデータ等を使用できる。メディア鍵は、光ディスク１に必ず記録されるが、ドライブシステムにとって既知の固定値は光ディスク１に記録する必要がない。上述したＴＯＣ中の所定のデータを固定値とする場合では、ＴＯＣデータ自身がドライブによって記録されるので、殊更、固定値を記録する必要はない。

【００２７】メディア鍵を光ディスク１に記録するために、ゲート１６は、セレクタ１２がメディア鍵を選択する時にオンするように、セレクト信号によって制御される。セレクタ１２が固定値を選択する時には、ゲート１６がオフとされる。ゲート１６の出力が記録回路１９に供給される。

【００２８】マルチプレクサ６は、暗号化されたコンテンツデータ、暗号化されたコンテンツ鍵およびＤＲＭ、

並びに変換されたアプリケーション鍵を所定のデータフォーマットに変換する。マルチプレクサ６の出力データがエラー訂正符号化器１７に供給される。エラー訂正符号化器１７によってエラー訂正符号化の処理がなされる。エラー訂正符号化器１７の出力が変調部１８で変調される。例えばＥＦＭ変調の処理がなされる。変調部１８の出力が記録回路１９に供給される。

【００２９】記録回路１９に対してゲート１６から出力されるメディア鍵とセレクタ１２を制御するセレクト信号とが供給される。記録回路１９では、フレーム同期信号、アドレス等の付加の処理を行い、また、メディア鍵およびセレクト信号がそれぞれ記録データに変換される。例えばＥＦＭ変調における結合ビット（３ビット）を利用してメディア鍵が光ディスク１に対して記録される。この場合では、メディア鍵を変調部１８に供給するようにしても良い。また、リードインエリアのＴＯＣの一部のデータとしてセレクト信号に基づいて生成されたタイプ識別子が記録される。さらに、記録回路１９のレーザドライバでは、光ディスク１に対して記録データを記録するための所定のレベルを有するドライブ信号が生成される。レーザドライバの出力が光ピックアップ３の半導体レーザに対して供給され、半導体レーザからドライブ信号に基づいて変調されたレーザ光が光ディスク１に照射され、データが記録される。

【００３０】図２は、この発明が適用され、図１の記録系に対応する再生系の構成の一例を示す。光ディスク１に光ピックアップ３から再生に必要とされるレーザ光を照射し、光ピックアップ３に設けられた４分割フォトディテクタによって光ディスク１によって反射されたレーザ光を決定する。検出された信号がＲＦ処理ブロック２１に供給される。ＲＦ処理ブロック２１では、マトリックスアンプがフォトディテクタの検出信号を演算することによって、再生（ＲＦ）信号、トラッキングエラー信号、フォーカスエラー信号を生成する。ウォブリンググルーブの情報としてクロックおよびアドレスが記録されている場合では、ウォブル信号がＲＦ処理ブロック２１から出力される。なお、記録系と同様に再生系も、専用のハードウエアに限らず、パーソナルコンピュータとソフトウェアによって実現することが可能である。

【００３１】ＲＦ信号が復調部２２に供給され、例えばＥＦＭ復調がなされる。復調部２２の出力データがエラー訂正回路２３に供給され、エラー訂正処理がなされる。エラー訂正回路２３の出力信号がデマルチプレクサ２４およびタイプＩＤ（識別子）読取部２５に供給される。図示しないサーボ回路に対して、トラッキングエラー信号、フォーカスエラー信号が供給され、スピンドルモータ２の回転および光ピックアップ３のトラッキングおよびフォーカスが制御される。サーボ回路は、光ピックアップ３に対するトラッキングサーボおよびフォーカスサーボと、スピンドルモータ２に対するスピンドルサーボと、スレッドサーボを行う。また、ウォブル信号を復調することによってアドレス情報が取り出される。このアドレス情報は、ＡＴＩＰ(Absolute Time In Pre-groove)と称され、時間情報によってディスク上の絶対アドレスを示すものである。アドレス情報は、システムコントローラ（図示しない）に供給され、光ディスク１上の所望のアドレスの情報を読み取るようになされる。

【００３２】デマルチプレクサ２４は、暗号化されたコンテンツデータ、暗号化されたコンテンツ鍵およびＤＲＭ、並びに変換されたアプリケーション鍵を分離して出力する。暗号化されたコンテンツデータが暗号化の復号を行うデクリプタ２６に供給される。デクリプタ２６によって暗号化が復号され、出力端子２７には、光ディスク１から再生され、復号されたコンテンツデータが取り出される。

【００３３】デマルチプレクサ２４で分離された暗号化されたコンテンツ鍵およびＤＲＭがデクリプタ２８に供給され、変換されたアプリケーション鍵が逆変換部２９に供給される。逆変換部２９は、記録系（図１参照）の変換部１４でなされた変換処理と逆の処理を行なうものである。例えば記録系でアプリケーション鍵に対してスクランブル処理が施される場合では、逆変換部２９では、デスクランブル処理がなされる。逆変換部２９から出力されるアプリケーション鍵がハッシュ演算部３０に供給される。

【００３４】ハッシュ演算部３０には、セレクタ３１の出力も供給されている。セレクタ３１の一方の入力端子ａには、デマルチプレクサ２４から出力される固定値が供給され、その他方の入力端子ｂには、ＲＦ処理ブロック２１で分離されたメディア鍵が供給される。固定値は、例えばＴＯＣの一部に記録されている特定のデータである。デマルチプレクサ２４は、固定値を分離して出力する。デマルチプレクサ２４が固定値を発生し、発生した固定値を出力するようにしても良い。

【００３５】メディア鍵は、光ディスク１（タイプＢ）にバインドしている鍵であり、外部から知ることが殆ど不可能なように、秘密に光ディスク１に記録されている。光ディスク１がタイプＡのディスクであれば、メディア鍵が記録されていない。セレクタ３１は、タイプＩＤ読取部２５から出力されるタイプＩＤによって制御される。

【００３６】タイプＩＤは、例えば光ディスク１の最内周部のＴＯＣの一部のデータとして記録される。光ディスク１をドライブに装着した場合、最初にＴＯＣ領域の情報が読み出される。タイプＩＤがタイプＡのディスクを示している場合では、入力端子ａが選択され、デマルチプレクサ２４からの固定値がハッシュ演算部３０に供給される。タイプＩＤがタイプＢのディスクを示している場合では、入力端子ｂが選択され、ＲＦ処理ブロック２１からのメディア鍵がハッシュ演算部３０に供給され

る。ハッシュ演算部３０が二つの入力のハッシュ値を求める。求められたハッシュ値がロッカー鍵である。

【００３７】ハッシュ演算部３０からのロッカー鍵がデクリプタ２８に供給される。デクリプタ２８によって、コンテンツ鍵およびＤＲＭに対して施されている暗号化が復号される。デクリプタ２８に接続されたデマルチプレクサ３２は、コンテンツ鍵と、ＤＲＭとを分離して出力する。コンテンツ鍵が上述したデクリプタ２６に供給され、コンテンツデータの暗号化が復号される。ＤＲＭが出力端子３３に取り出される。

【００３８】図３は、タイプ判別とセレクタ３１の制御動作の流れを示すフローチャートである。最初のステップＳ１において、タイプＩＤの読取がなされる。読み取られたタイプＩＤに基づいて、再生しようとする光ディスク１がタイプＡか否かがステップＳ２において判定される。タイプＡのディスクであると判定されると、デマルチプレクサ２４からの固定値をセレクタ３１が選択的に出力する（ステップＳ３）。図３の例では、全て"1"の１２８ビットのデータを固定値として使用する例が示されている。

【００３９】タイプＡのディスクでないと、ステップＳ２で判定された場合では、ステップＳ４において、タイプＢのディスクであるか否かが判定される。タイプＢのディスクと決定されるならば、ステップＳ５においてメディア鍵の読取がなされる。そして、読み取られたメディア鍵がステップＳ６においてセレクタ３１から出力される。若し、ステップＳ４において、タイプＢのディスクでないと判定されると、タイプＡおよびＢの何れでもないとの判定結果となる。この場合は、エラー処理がなされる（ステップＳ７）。

【００４０】上述したこの発明の一実施形態において、メディアにバインドしていない固定値を使用している場合では、全く同一のコピーメディアが作成可能となるので、著作権保護が不十分となる。この影響を軽減するために、固定値を使用したタイプＡのディスクの場合では、再生環境を制限することが好ましい。例えばタイプＡのディスクでは、コンテンツデータをその光ディスクに記録したソフトウェアまたはハードウエアのＩＤ（識別子）をディスクに記録し、そのＩＤを共有している装置のみがそのコンテンツデータを再生できるようになされる。極端な例は、記録を行なったドライブまたはソフトウェアのみがその光ディスクを再生することが可能とされる。一方、メディア鍵を使用している場合では、再生環境を制限しないようになされる。

【００４１】この発明は、上述したこの発明の一実施形態等に限定されるものでは無く、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えば使用する光ディスクとして、タイプＡおよびＢ以外の第３のタイプのものを使用しても良い。第３のタイプの光ディスクは、読み出し専用エリアにその光ディスク固有の識別情報が記録されたものである。そして、この識別情報を使用して求めたハッシュ値を鍵データとして暗号化がなされる。第３のタイプの光ディスクの記録および／または再生を可能とするようにしても良い。また、この発明は、書き換え可能形光ディスク、追記形光ディスク以外に読み出し専用形光ディスクに対しても適用することができる。読み出し専用形の場合では、図１に示す記録装置は、マスタリング装置に対して適用される。さらに、この発明は、光ディスク限らず、他のデータ記録媒体例えばメモリカードに対しても適用することができる。

【００４２】

【発明の効果】この発明では、メディアにバインドしているメディア鍵を使用した本格的なセキュリティ機能を実現する新規なドライブが普及していない段階では、本格的なセキュリティ機能との互換性を有する、固定値を使用したセキュリティ機能を実現することによって、新規なドライブをスムーズに導入することが可能となる。また、メディアにバインドしているか否かをタイプＩＤで識別することによって、メディア鍵を使用したセキュリティ機能と固定値を使用したセキュリティ機能とを同じセキュリティシステム上でハンドリングすることができ、互換性を容易にとることができる。さらに、メディアにバインドしていない固定値を使用した場合でも、再生環境を制限することによって、セキュリティを保持することができる。

【図面の簡単な説明】

【図１】この発明の一実施形態における記録装置の構成例を示すブロック図である。

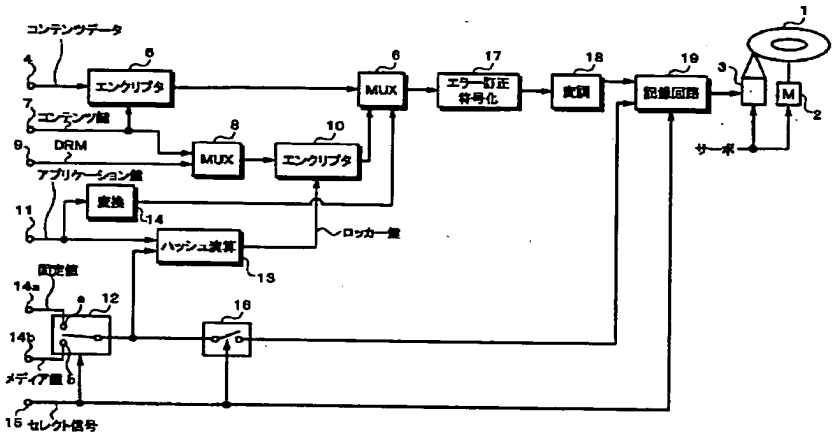
【図２】この発明の一実施形態における再生装置の構成例を示すブロック図である。

【図３】この発明の一実施形態におけるタイプ識別動作の処理の流れを示すフローチャートである。

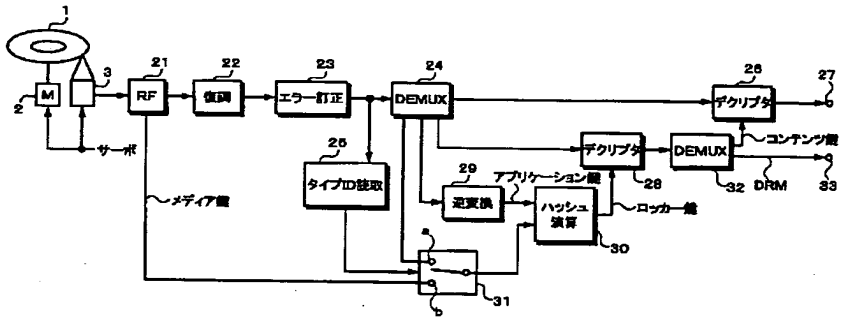
【符号の説明】

１・・・光ディスク、３・・・光ピックアップ、５、１０・・・エンクリプタ、７・・・コンテンツ鍵の入力端子、１２・・・セレクタ、１３・・・ハッシュ演算部、１４ａ・・・固定値の入力端子、１４ｂ・・・メディア鍵の入力端子、１５・・・セレクト信号の入力端子

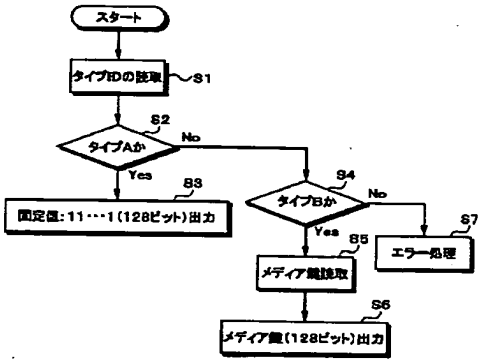
【図１】


コンテンツデータ
エンクリプタ
MUX
エラー訂正符号化
変調
記録回路
コンテンツ鍵
DRM
アプリケーション鍵
変換
ハッシュ演算
ロッカー鍵
固定値
メディア鍵
セレクト信号
サーボ

【図２】


RF
復調
エラー訂正
DEMUX
デクリプタ
タイプID読取
逆変換
アプリケーション鍵
ハッシュ演算
ロッカー鍵
コンテンツ鍵
DRM
メディア鍵
サーボ

【図３】


スタート
タイプIDの読取
S1
タイプAか
S2
No
Yes
固定値:11…1(128ビット)出力
S3
タイプBか
S4
No
Yes
エラー処理
S7
メディア鍵読取
S5
メディア鍵(128ビット)出力
S6

フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/08	Ｈ０４Ｌ	9/00	６０１Ｚ
// Ｈ０４Ｎ	5/91	Ｈ０４Ｎ	5/91	Ｐ

(72)発明者　古川　俊介
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5C053 FA13 FA23 GB15 JA21 LA06
5D044 AB05 BC05 BC06 CC06 DE02
DE03 DE12 DE49 DE50 DE53
DE57 DE58 EF05 FG18 GK12
GK17
5J104 AA16 EA06 EA17 NA02 NA12
PA14

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１５年６月２０日（２００３．６．２０）

【公開番号】特開２００３－３７５８９（Ｐ２００３－３７５８９Ａ）
【公開日】平成１５年２月７日（２００３．２．７）
【年通号数】公開特許公報１５－３７６
【出願番号】特願２００１－２２６２４２（Ｐ２００１－２２６２４２）
【国際特許分類第７版】
H04L 9/14
G11B 20/10
311
321
H04L 9/08
// H04N 5/91
【ＦＩ】
H04L 9/00 641
G11B 20/10 D
H
311
321 Z
H04L 9/00 601 Z
H04N 5/91 P

【手続補正書】
【提出日】平成１５年３月４日（２００３．３．４）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正内容】
【発明の名称】 記録媒体の記録装置および方法、記録媒体の再生装置および方法、並びに記録媒体
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】 入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理を施す暗号化処理部と、
上記暗号化処理部からの出力データにエンコード処理を施すとともに、上記暗号化処理部で上記記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込むエンコード処理部と、
上記エンコード処理部からの出力データを記録媒体に記録する記録部とを備えている記録媒体の記録装置。
【請求項２】 上記暗号化処理部は、上記入力されたコンテンツデータにコンテンツ鍵データを用いて暗号化処理を施すエンクリプタを備えている請求項１に記載の記録媒体の記録装置。
【請求項３】 上記暗号化処理部は、更に上記コンテンツ鍵データを上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データによって暗号化処理を行う更なるエンクリプタを備えている請求項２に記載の記録媒体の記録装置。
【請求項４】 上記更なるエンクリプタは、上記コンテンツ鍵データとともに上記コンテンツデータの著作権管理データを暗号化処理する請求項３に記載の記録媒体の記録装置。
【請求項５】 上記暗号化処理部は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データのいずれかのデータとアプリケーション鍵データとにより演算処理を行う演算処理部を備え、上記演算処理部からの出力データを上記更なるエンクリプタに暗号化処理のための鍵データとして供給する請求項３に記載の記録媒体の記録装置。
【請求項６】 上記エンクリプタからの出力データと上記アプリケーション鍵データと上記更なるエンクリプタからの出力データは、上記エンコード処理部に供給され

る請求項４に記載の記録媒体の記録装置。
【請求項７】　上記暗号化処理部は、更に上記アプリケーション鍵データを変換する変換回路部を備え、上記変換回路部からの出力データが上記エンコーダに供給される請求項６に記載の記録媒体の記録装置。
【請求項８】　上記装置は、上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データを上記記録媒体に記録する請求項１に記載の記録媒体の記録装置。
【請求項９】　入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理し、
上記暗号化処理されたデータにエンコード処理を施す際に、上記暗号化処理の際に上記記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込み、
上記エンコード処理されたデータを記録媒体に記録する記録媒体の記録方法。
【請求項１０】　上記方法は、上記入力されたコンテンツデータに先ずコンテンツ鍵データを用いて暗号化処理を施す請求項９に記載の記録媒体の記録方法。
【請求項１１】　上記方法は、更に上記コンテンツ鍵データを上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データによって暗号化処理を行う請求項１０に記載の記録媒体の記録方法。
【請求項１２】　上記方法は、上記コンテンツ鍵データとともに上記コンテンツデータの著作権管理データを上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データによって暗号化処理する請求項１１に記載の記録媒体の記録方法。
【請求項１３】　上記方法は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データのいずれかのデータとアプリケーション鍵データとにより演算処理を行い、上記演算処理の結果得られるデータを用いて上記コンテンツ鍵データを暗号化処理する請求項１１に記載の記録媒体の記録方法。
【請求項１４】　上記方法は、上記暗号化されたコンテンツデータと上記アプリケーション鍵データと上記暗号化されたコンテンツ鍵データとがエンコード処理される請求項１３に記載の記録媒体の記録方法。
【請求項１５】　上記方法は、上記アプリケーション鍵データは所定の変換処理が施されたあとにエンコード処理が施される請求項１４に記載の記録媒体の記録方法。
【請求項１６】　上記方法は、上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データを上記記録媒体に記録する請求項９に記載の記録媒体の記録方法。
【請求項１７】　コンテンツデータが暗号化されて記録されている記録媒体からデータを読み出すヘッド部と、
上記ヘッド部からの信号にデコード処理を施すデコーダと、
上記記録媒体から読み出された上記記録媒体に記録されることによって記録媒体専用の鍵データとなる鍵データ又は固定値データのいずれかを用いて上記デコーダからの出力データに施されている暗号を解く解読処理部とを備えている記録媒体の再生装置。
【請求項１８】　上記解読処理部は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データとのいずれかのデータと上記記録媒体から読み出されたアプリケーション鍵データとを用いて上記デコーダの出力データからコンテンツ鍵データを取り出すディクリプタとを備えている請求項１７に記載の記録媒体の再生装置。
【請求項１９】　上記解読処理部は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データとのいずれかのデータと上記記録媒体から読み出されたアプリケーション鍵データとを用いて演算処理を行い、上記演算処理の結果得られるデータを上記ディクリプタに暗号解読の鍵データとして供給する演算処理部を備えている請求項１８に記載の記録媒体の再生装置。
【請求項２０】　上記装置は、更に上記演算処理部に上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データとのいずれかのデータを選択的に供給する選択処理部を備えている請求項１９に記載の記録媒体の再生装置。
【請求項２１】　上記記録媒体には、上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データが記録されており、
上記装置は更に上記デコーダの出力データから上記識別データを読み取る読み取り部を備え、上記読み取り部からの出力データにより上記選択処理部が制御される請求項２０に記載の記録媒体の再生装置。
【請求項２２】　上記解読処理部は、更に上記デコーダの出力データに施されている暗号を上記コンテンツ鍵データを用いて解読する更なるディクリプタとを備えている請求項１８に記載の記録媒体の再生装置。
【請求項２３】　コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号されて記録されているとともに、上記コンテンツデータが上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データが記録された記録媒体から上記識別データを読み出し、
上記読み出された識別データによって上記コンテンツデ

ータが上記固定値データによって暗号化処理されていると判別されたときには、上記記録媒体から読み出されたデータを上記固定値データによって暗号の解読処理を行い、
上記読み出された識別データによって上記コンテンツデータが上記記録されることによって記録媒体専用の鍵データとなる鍵データによって暗号化されていると判別されたときには、上記記録媒体から読み出されたコンテンツデータを上記記録媒体から読み出された上記記録されることによって記録媒体専用の鍵データとなる鍵データとを用いて暗号の解読処理を行う記録媒体の再生方法。
【請求項２４】　上記方法は、上記記録媒体が上記コンテンツデータが上記記録されることによって記録媒体専用の鍵データとなる鍵データで暗号化されて記録された記録媒体か、上記固定値データを用いて上記コンテンツデータが暗号化されて記録された記録媒体のいずれでもない場合には再生処理を中止する請求項２３に記載の記録媒体の再生方法。
【請求項２５】　暗号化されたコンテンツデータが記録されるデータ領域と、
上記データ領域に先立って読み出される位置に設けられ、上記データ領域の管理データと、上記コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データとを含むデータが記録される管理データ領域とを備えている記録媒体。
【請求項２６】　上記管理データ領域には、上記固定値データが記録されている請求項２５に記載の記録媒体。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００１
【補正方法】変更
【補正内容】
【０００１】
【発明の属する技術分野】この発明は、暗号化によってセキュリティを保つようにしたデータを記録する記録媒体の記録装置および方法、記録媒体の再生装置および方法、並びに記録媒体に関する。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００６
【補正方法】変更
【補正内容】
【０００６】したがって、この発明の目的は、メディアにバインドした鍵を使用して暗号化する本格的なセキュリティ機能の導入を容易とすることが可能な記録媒体の記録装置および方法、記録媒体の再生装置および方法、並びに記録媒体を提供することにある。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正内容】
【０００７】
【課題を解決するための手段】上述した課題を達成するために、請求項１の発明は、入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理を施す暗号化処理部と、暗号化処理部からの出力データにエンコード処理を施すとともに、暗号化処理部で記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込むエンコード処理部と、エンコード処理部からの出力データを記録媒体に記録する記録部とを備えている記録媒体の記録装置である。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正内容】
【０００８】請求項９の発明は、入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理し、暗号化処理されたデータにエンコード処理を施す際に、暗号化処理の際に記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込み、エンコード処理されたデータを記録媒体に記録する記録媒体の記録装置である。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】変更
【補正内容】
【０００９】請求項１７の発明は、コンテンツデータが暗号化されて記録されている記録媒体からデータを読み出すヘッド部と、ヘッド部からの信号にデコード処理を施すデコーダと、記録媒体から読み出された記録媒体に記録されることによって記録媒体専用の鍵データとなる鍵データ又は固定値データのいずれかを用いてデコーダからの出力データに施されている暗号を解く解読処理部とを備えている記録媒体の再生装置である。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】変更
【補正内容】
【００１０】コンテンツデータが記録されることによっ

て記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号されて記録されているとともに、コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データが記録された記録媒体から識別データを読み出し、読み出された識別データによってコンテンツデータが固定値データによって暗号化処理されていると判別されたときには、記録媒体から読み出されたデータを固定値データによって暗号の解読処理を行い、読み出された識別データによってコンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データによって暗号化されていると判別されたときには、記録媒体から読み出されたコンテンツデータを記録媒体から読み出された記録されることによって記録媒体専用の鍵データとなる鍵データとを用いて暗号の解読処理を行う記録媒体の再生方法である。請求項２５の発明は、暗号化されたコンテンツデータが記録されるデータ領域と、データ領域に先立って読み出される位置に設けられ、データ領域の管理データと、コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データとを含むデータが記録される管理データ領域とを備えている記録媒体である。